GOVERNMENT OF INDIA
ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA

UNSTARRED QUESTION NO:1099
ANSWERED ON:08.02.2017
Cyber-Crime/Stalking
Chaudhury Shri Jitendra;Choubey Shri Ashwini Kumar

Will the Minister of ELECTRONICS AND INFORMATION TECHNOLOGY be pleased to state:

Will the Minister of ELECTRONICS AND INFORMATION TECHNOLOGY be please to state:

(a) whether it is fact that cybercrime is increasing day by day in all over the country;
(b) if so, the details thereof;
(c) whether harassment and blackmailing case particularly of women by cyber stalkers are increasing through social sites;
(d) if so, the details thereof; and
(e) the action Government has taken and proposes to take in this regard?

Answer

(a) and (b): With the proliferation of Information Technology and related services there is a rise in instances of cyber crimes in the country like elsewhere in the world.
- As per the data maintained by National Crime Records Bureau (NCRB), a total of 5693, 9622 and 11592 cyber crime cases were registered during the years 2013, 2014 and 2015 respectively, showing a rise of 69% during 2013 to 2014 and 20% during 2014 to 2015. This includes cases registered under the IT Act and related sections of Indian Penal Code and special & local laws involving computer as medium/ target.
- As per the information reported to and tracked by Indian Computer Emergency Response Team (CERT-In), a total no. of 44679, 49455 and 50362 cyber security incidents were observed during the year 2014, 2015 and 2016 respectively. The types of cyber security incidents include phishing, scanning/probing, website intrusions and defacements, virus/malicious code, Denial of Service attacks, etc.
- RBI has registered a total of 9500, 13083, 16468, and 8689 cases of frauds involving credit cards, ATM / debit cards and internet banking during the year 2013-14, 2014-15, 2015-16 and 2016-17(upto December 2016), respectively.
- Further, CBI has registered a total of 87 cases during 2014 to 2016. Out of these 87 cases, charge-sheets have been filed in 36 cases, status report filed in competent court in 4 cases, 6 cases were closed and 41 cases are under investigation by CBI.

(c) and (d): Police and public order are State subjects under the Constitution and as such the State Governments and Union Territory Administrations are primarily responsible for prevention, detection, registration and investigation of crimes including harassment and blackmailing of women (Crime against Women) and for prosecuting the criminals through Law Enforcement machinery within their jurisdictions. NCRB collects and maintains statistical data of police recorded cognizable crimes from 35 States /Union Territories. As per the data maintained by NCRB under stalking on women (section 354D IPC) during 2014-2015, a total of 4699 and 6266 cases were registered during the year 2014 and 2015, respectively, showing a rise of 25% during 2014 to 2015.

(e) The Social media sites are being used by the citizens across the world through Internet. At times, Social media is also used by anti-national/anti-social elements. Government does not regulate the content appearing on social networking sites. However,

- The Information Technology (IT) Act, 2000 has provisions for removal of objectionable online content. The Information Technology (Intermediary Guidelines) Rules 2011 under section 79 of the IT Act requires that the Intermediaries shall observe due diligence while discharging their duties and shall inform the users of computer resources not to host, display, upload, modify, publish, transmit, update or share any information that is harmful, objectionable, affects minors or is unlawful in any way. Action is taken as and when incidents are brought to the knowledge of Law Enforcement Agencies.

- Government takes action under section 69A of IT Act for blocking of websites/webpages with objectionable content, whenever requests are received from designated nodal officers or upon Court orders. Section 69A of the IT Act empowers Government to block any information generated, transmitted, received, stored or hosted in any computer resource in the interest of i) sovereignty and integrity of India, ii) defence of India, iii) security of the State, iv) friendly relations with foreign States, v) public order, or, vi) for preventing incitement to the commission of any cognizable offence relating to above.

- The Government has also mandated all the Telecom Service Providers including Internet Service Providers to provide the Lawful Interception facilities to the security agencies for all the services including WhatsApp, Viber, etc. Thus security agencies are able to intercept these encrypted communication services through the lawful interception facilities provided by the Telecom Service

Providers, but they are not able to decrypt some of the encrypted intercepted communication to readable format.
******